Vulnerability Summary for the Week of June 28, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 07/05/2021 12:11 PM EDT

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of June 28, 2021

07/05/2021 07:06 AM EDT

Original release date: July 5, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- after_effects	Adobe After Effects version 18.1 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An unauthenticated attacker could exploit this to to plant custom binaries and execute them with System permissions. Exploitation of this issue requires user interaction.	2021-06-28	9.3	CVE-2021-28570 MISC
adobe -- after_effects	After Effects version 18.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	9.3	CVE-2021-28586 MISC
adobe -- robohelp_server	Adobe RoboHelp Server version 2019.0.9 (and earlier) is affected by a Path Traversal vulnerability when parsing a crafted HTTP POST request. An authenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	2021-06-28	9	CVE-2021-28588 MISC
chamilo -- chamilo	main/inc/ajax/model.ajax.php in Chamilo through 1.11.14 allows SQL Injection via the searchField, filters, or filters2 parameter.	2021-06-28	7.5	CVE-2021-34187 MISC MISC MISC MISC
cnesty -- helpcom	A vulnerability of Helpcom could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient validation of the parameter. This issue affects: Cnesty Helpcom 10.0 versions prior to.	2021-06-29	7.5	CVE-2020-7871 MISC
eclipse -- birt	In Eclipse BIRT versions 4.8.0 and earlier, an attacker can use query parameters to create a JSP file which is accessible from remote (current BIRT viewer dir) to inject JSP code into the running instance.	2021-06-25	7.5	CVE-2021-34427 CONFIRM
fatek -- winproladder	FATEK Automation WinProladder Versions 3.30 and prior do not properly restrict operations within the bounds of a memory buffer, which may allow an attacker to execute arbitrary code.	2021-06-29	7.5	CVE-2021-32992 MISC
fatek -- winproladder	FATEK Automation WinProladder Versions 3.30 and prior are vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code.	2021-06-29	7.5	CVE-2021-32988 MISC
fatek -- winproladder	FATEK Automation WinProladder Versions 3.30 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	2021-06-29	7.5	CVE-2021-32990 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fidelissecurity -- deception	Vulnerability in the CommandPost, Collector, and Sensor components of Fidelis Network and Deception enables an attacker with user level access to the CLI to inject root level commands into the component and neighboring Fidelis components. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.	2021-06-25	9	CVE-2021-35047 CONFIRM
fidelissecurity -- deception	Vulnerability in Fidelis Network and Deception CommandPost enables unauthenticated SQL injection through the web interface. The vulnerability could lead to exposure of authentication tokens in some versions of Fidelis software. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.	2021-06-25	7.5	CVE-2021-35048 CONFIRM
helpu -- helpu	A remote code execution vulnerability exists in helpUS(remote administration tool) due to improper validation of parameter of ShellExecutionExA function used for login.	2021-06-29	10	CVE-2020-7868 MISC
huawei -- anyoffice	There is a deserialization vulnerability in Huawei AnyOffice V200R006C10. An attacker can construct a specific request to exploit this vulnerability. Successfully exploiting this vulnerability, the attacker can execute remote malicious code injection and to control the device.	2021-06-29	9.3	CVE-2021-22439 MISC
inkdrop -- inkdrop	Inkdrop versions prior to v5.3.1 allows an attacker to execute arbitrary OS commands on the system where it runs by loading a file or code snippet containing an invalid iframe into Inkdrop.	2021-06-28	9.3	CVE-2021-20745 MISC MISC MISC
mastersoft -- zook	An improper input validation vulnerability of ZOOK software (remote administration tool) could allow a remote attacker to create arbitrary file. The ZOOK viewer has the "Tight file CMD" function to create file. An attacker could create and execute arbitrary file in the ZOOK agent program using "Tight file CMD" without authority.	2021-06-29	9	CVE-2020-7869 MISC
mcafee -- mvision_edr	A command injection vulnerability in MVISION EDR (MVEDR) prior to 3.4.0 allows an authenticated MVEDR administrator to trigger the EDR client to execute arbitrary commands through PowerShell using the EDR functionality 'execute reaction'.	2021-06-29	9	CVE-2021-31838 CONFIRM
miniaudio_project -- miniaudio	Miniaudio 0.10.35 has a Double free vulnerability that could cause a buffer overflow in ma_default_vfs_close__stdio in miniaudio.h.	2021-06-25	7.5	CVE-2021-34184 CONFIRM
misp -- misp	app/View/Elements/genericElements/IndexTable/Fields/generic_field.ctp in MISP 2.4.144 does not sanitize certain data related to generic-template:index.	2021-06-25	7.5	CVE-2021-35502 MISC
narou_project -- narou	Narou (aka Narou.rb) before 3.8.0 allows Ruby Code Injection via the title name or author name of a novel.	2021-06-28	7.5	CVE-2021-35514 MISC MISC
naviwebs -- navigate_cms	SQL Injection vulnerability in NavigateCMS 2.9 via the URL encoded GET input category in navigate.php.	2021-06-28	7.5	CVE-2020-23711 MISC
online_pet_shop_web_application_project -- online_pet_shop_web_application	Online Pet Shop We App 1.0 is vulnerable to remote SQL injection and shell upload	2021-06-28	7.5	CVE-2021-35456 MISC MISC
pandorafms -- pandora_fms	PandoraFMS <=7.54 allows arbitrary file upload, it leading to remote command execution via the File Manager. To bypass the built-in protection, a relative path is used in the requests.	2021-06-25	7.5	CVE-2021-34074 MISC
phoenixcontact -- axl_f_bk_pn_tps_xc_firmware	In certain devices of the Phoenix Contact AXL F BK and IL BK product families an undocumented password protected FTP access to the root directory exists.	2021-06-25	7.5	CVE-2021-33540 CONFIRM
phoenixcontact -- fl_switch_smcs_16tx_firmware	In Phoenix Contact FL SWITCH SMCS series products in multiple versions if an attacker sends a hand-crafted TCP-Packet with the Urgent-Flag set and the Urgent-Pointer set to 0, the network stack will crash. The device needs to be rebooted afterwards.	2021-06-25	7.8	CVE-2021-21005 CONFIRM
phoenixcontact -- ilc1x0_firmware	Phoenix Contact Classic Line Controllers ILC1x0 and ILC1x1 in all versions/variants are affected by a Denial-of-Service vulnerability. The communication protocols and device access do not feature authentication measures. Remote attackers can use specially crafted IP packets to cause a denial of service on the PLC's network communication module. A successful attack stops all network communication. To restore the network connectivity the device needs to be restarted. The automation task is not affected.	2021-06-25	7.8	CVE-2021-33541 CONFIRM
securepoint -- openvpn-client	Securepoint SSL VPN Client v2 before 2.0.32 on Windows has unsafe configuration handling that enables local privilege escalation to NT AUTHORITY\SYSTEM. A non-privileged local user can modify the OpenVPN configuration stored under "%APPDATA%\Securepoint SSL VPN" and add a external script file that is executed as privileged user.	2021-06-28	7.2	CVE-2021-35523 MISC MISC FULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- nessus	Nessus versions 8.13.2 and earlier were found to contain a privilege escalation vulnerability which could allow a Nessus administrator user to upload a specially crafted file that could lead to gaining administrator privileges on the Nessus host.	2021-06-29	7.2	CVE-2021-20079 MISC
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable use of hard-coded credentials vulnerability exists in multiple iw_* utilities. The device operating system contains an undocumented encryption password, allowing for the creation of custom diagnostic scripts. An attacker can send diagnostic scripts while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33531 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable privilege escalation vulnerability exists in the iw_console functionality. A specially crafted menu selection string can cause an escape from the restricted console, resulting in system access as the root user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33528 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in encrypted diagnostic script functionality of the devices. A specially crafted diagnostic script file can cause arbitrary busybox commands to be executed, resulting in remote control over the device. An attacker can send diagnostic while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33530 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the hostname functionality. A specially crafted entry to network configuration information can cause execution of arbitrary system commands, resulting in full control of the device. An attacker can send various requests while authenticated as a high privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33534 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the iw_webs functionality. A specially crafted diagnostic script file name can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33532 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the iw_webs functionality. A specially crafted iw_serverip parameter can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33533 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable improper access control vulnerability exists in the iw_webs account settings functionality. A specially crafted user name entry can cause the overwrite of an existing user account password, resulting in remote shell access to the device as that user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33538 CONFIRM
wincred_project -- wincred	This affects all versions of package wincred. If attacker-controlled user input is given to the getCredential function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-06-28	7.5	CVE-2021-23399 MISC MISC
zohocorp -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus through 6101 is vulnerable to unauthenticated Remote Code Execution while changing the password.	2021-06-25	7.5	CVE-2021-28958 MISC MISC
zohocorp -- manageengine_servicedesk_plus_msp	Zoho ManageEngine ServiceDesk Plus MSP before 10521 is vulnerable to Server-Side Request Forgery (SSRF).	2021-06-29	7.5	CVE-2021-31531 CONFIRM MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- after_effects	After Effects versions 18.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	4.3	CVE-2021-28587 MISC
adobe -- animate	Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	4.3	CVE-2021-28573 MISC
adobe -- connect	Adobe Connect version 11.2.1 (and earlier) is affected by an Improper access control vulnerability that can lead to the elevation of privileges. An attacker with 'Learner' permissions can leverage this scenario to access the list of event participants.	2021-06-28	4	CVE-2021-28579 MISC
adobe -- experience_manager	AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by an Improper Access Control vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service in the context of the current user.	2021-06-28	5	CVE-2021-21083 MISC
adobe -- experience_manager	AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2021-06-28	4.3	CVE-2021-21084 MISC
apache -- traffic_server	Improper Input Validation vulnerability in HTTP/2 of Apache Traffic Server allows an attacker to DOS the server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-30	5	CVE-2021-32567 MISC
apache -- traffic_server	Improper Input Validation vulnerability in HTTP/2 of Apache Traffic Server allows an attacker to DOS the server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-30	5	CVE-2021-32566 MISC
auth0 -- nextjs-auth0	The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. Versions before and including `1.4.1` are vulnerable to reflected XSS. An attacker can execute arbitrary code by providing an XSS payload in the `error` query parameter which is then processed by the callback handler as an error message. You are affected by this vulnerability if you are using `@auth0/nextjs-auth0` version `1.4.1` or lower **unless** you are using custom error handling that does not return the error message in an HTML response. Upgrade to version `1.4.1` to resolve. The fix adds basic HTML escaping to the error message and it should not impact your users.	2021-06-25	4.3	CVE-2021-32702 MISC CONFIRM MISC
autodesk -- advance_steel	A maliciously crafted DWG file can be forced to read beyond allocated boundaries when parsing the DWG file. This vulnerability can be exploited to execute arbitrary code.	2021-06-25	6.8	CVE-2021-27040 MISC
autodesk -- advance_steel	A maliciously crafted DWG file can be used to write beyond the allocated buffer while parsing DWG files. This vulnerability can be exploited to execute arbitrary code.	2021-06-25	6.8	CVE-2021-27041 MISC
autodesk -- advance_steel	A maliciously crafted DWG file can be used to write beyond the allocated buffer while parsing DWG files. The vulnerability exists because the application fails to handle a crafted DWG file, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code.	2021-06-25	6.8	CVE-2021-27042 MISC
autodesk -- advance_steel	An Arbitrary Address Write issue in the Autodesk DWG application can allow a malicious user to leverage the application to write in unexpected paths. In order to exploit this the attacker would need the victim to enable full page heap in the application.	2021-06-25	4.3	CVE-2021-27043 MISC
avaya -- aura_device_services	An arbitrary code execution vulnerability was discovered in Avaya Aura Device Services that may potentially allow a local user to execute specially crafted scripts. Affects 7.0 through 8.1.4.0 versions of Avaya Aura Device Services.	2021-06-25	4.6	CVE-2021-25654 MISC
cisco -- dna_center	A vulnerability in the Cisco Identity Services Engine (ISE) integration feature of the Cisco DNA Center Software could allow an unauthenticated, remote attacker to gain unauthorized access to sensitive data. The vulnerability is due to an incomplete validation of the X.509 certificate used when establishing a connection between DNA Center and an ISE server. An attacker could exploit this vulnerability by supplying a crafted certificate and could then intercept communications between the ISE and DNA Center. A successful exploit could allow the attacker to view and alter sensitive information that the ISE maintains about clients that are connected to the network.	2021-06-29	5.8	CVE-2021-1134 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
crmeb -- crmeb	SQL Injection vulnerability in Zhong Bang Technology Co., Ltd CRMEB mall system V2.60 and V3.1 via the tablename parameter in SystemDatabackup.php.	2021-06-29	6.5	CVE-2020-21394 MISC
dovecot -- dovecot	The Sieve engine in Dovecot before 2.3.15 allows Uncontrolled Resource Consumption, as demonstrated by a situation with a complex regular expression for the regex extension.	2021-06-28	4	CVE-2020-28200 MISC CONFIRM
dovecot -- dovecot	The submission service in Dovecot before 2.3.15 allows STARTTLS command injection in lib-smtp. Sensitive information can be redirected to an attacker-controlled address.	2021-06-28	5.8	CVE-2021-33515 MISC CONFIRM
enhancesoft -- osticket	Cross Site Scripting vulnerability in Enhancesoft osTicket before v1.12.6 via the queue-name parameter to include/ajax.search.php.	2021-06-28	4.3	CVE-2020-22608 CONFIRM
enhancesoft -- osticket	Cross Site Scripting (XSS) vulnerability in Enhancesoft osTicket before v1.12.6 via the queue-name parameter in include/class.queue.php.	2021-06-28	4.3	CVE-2020-22609 CONFIRM
fidelissecurity -- deception	User credentials stored in a recoverable format within Fidelis Network and Deception CommandPost. In the event that an attacker gains access to the CommandPost, these values could be decoded and used to login to the application. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.3. This vulnerability has been addressed in version 9.3.3 and subsequent versions.	2021-06-25	5	CVE-2021-35050 CONFIRM
fidelissecurity -- deception	Vulnerability in Fidelis Network and Deception CommandPost enables authenticated command injection through the web interface. The vulnerability could allow a specially crafted HTTP request to execute system commands on the CommandPost and return results in an HTTP response in an authenticated session. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.	2021-06-25	6.5	CVE-2021-35049 CONFIRM
google -- bindiff	An attacker can craft a specific IdaPro *.i64 file that will cause the BinDiff plugin to load an invalid memory offset. This can allow the attacker to control the instruction pointer and execute arbitrary code. It is recommended to upgrade BinDiff 7	2021-06-29	4.6	CVE-2021-22545 MISC
huawei -- ecns280_firmware	There is an XXE injection vulnerability in eCNS280 V100R005C00 and V100R005C10. A module does not perform the strict operation to the input XML message. Attacker can send specific message to exploit this vulnerability, leading to the module denial of service.	2021-06-29	5	CVE-2021-22338 MISC
huawei -- emui	There is an Information Disclosure Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause out-of-bounds read.	2021-06-30	6.4	CVE-2021-22354 MISC
huawei -- ips_module_firmware	There is a memory leak vulnerability in Huawei products. A resource management weakness exists in a module. Attackers with high privilege can exploit this vulnerability by performing some operations. This can lead to memory leak. Affected product versions include:IPS Module V500R005C00SPC100,V500R005C00SPC200;NGFW Module V500R005C00SPC100,V500R005C00SPC200;NIP6300 V500R005C00SPC100,V500R005C10SPC200;NIP6600 V500R005C00SPC100,V500R005C00SPC200;Secospace USG6300 V500R005C00SPC100,V500R005C00SPC200;Secospace USG6500 V500R005C00SPC100,V500R005C10SPC200;Secospace USG6600 V500R005C00SPC100,V500R005C00SPC200.	2021-06-29	4	CVE-2021-22341 MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow 19.0.03 and 20.0 and IBM Cloud Pak for Automation 20.0.3-IF002 and 21.0.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 203029.	2021-06-28	4.3	CVE-2021-29775 CONFIRM CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 4.0.0.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196212.	2021-06-28	5	CVE-2021-20413 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could be vulnerable to cross-site request forgery (CSRF) which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 198241.	2021-06-29	4.3	CVE-2021-20580 CONFIRM XF
ibm -- security_identity_manager_adapter	IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow the and cause the server to crash. IBM X-Force ID: 199249.	2021-06-28	4	CVE-2021-20573 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_identity_manager_adapter	IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow the and cause the server to crash. IBM X-Force ID: 199247.	2021-06-28	4	CVE-2021-20572 CONFIRM XF
ibm -- security_identity_manager_adapter	IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a heap based buffer overflow, caused by improper bounds. An authenticared user could overflow the buffer and cause the service to crash. IBM X-Force ID: 197882.	2021-06-28	4	CVE-2021-20494 CONFIRM XF
ibm -- security_verify	IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) could disclose sensitive information through an HTTP GET request by a privileged user due to improper input validation.. IBM X-Force ID: 199396.	2021-06-25	4	CVE-2021-20583 XF CONFIRM
ibm -- security_verify	IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) is vulnerable to link injection. By persuading a victim to click on a specially-crafted URL link, a remote attacker could exploit this vulnerability to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking	2021-06-25	5.8	CVE-2021-29676 XF CONFIRM
ibm -- security_verify_privilege_manager	IBM Security Sevret Server (IBM Security Verify Privilege Manager 10.8.2) could allow a local user to execute code due to improper integrity checks. IBM X-Force ID: 184919.	2021-06-25	4.6	CVE-2020-4610 XF CONFIRM
ibm -- security_verify_privilege_manager	IBM Security Sevret Server (IBM Security Verify Privilege Manager 10.8.2) is vulnerable to a buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and execute arbitrary code on the system or cause the system to crash. IBM X-Force ID: 184917.	2021-06-25	4.6	CVE-2020-4609 XF CONFIRM
imagemagick -- imagemagick	ImageMagick 7.0.11-14 has a memory leak in AcquireSemaphoreMemory in semaphore.c and AcquireMagickMemory in memory.c.	2021-06-25	5	CVE-2021-34183 CONFIRM
infoblox -- nios	Infoblox NIOS before 8.5.2 allows entity expansion during an XML upload operation, a related issue to CVE-2003-1564.	2021-06-28	4	CVE-2020-15303 MISC MISC
ipfire -- ipfire	Cross Site Scripting (XSS) vulnerabilty in IPFire 2.23 via the IPfire web UI in the mail.cgi.	2021-06-28	4.3	CVE-2020-21142 MISC
istio -- istio	Istio before 1.9.6 and 1.10.x before 1.10.2 has Incorrect Access Control.	2021-06-29	6.5	CVE-2021-34824 MISC MISC
limesurvey -- limesurvey	Cross Site Scripting vulnerabilty in LimeSurvey 4.1.11+200316 via the (1) name and (2) description parameters in application/controllers/admin/PermissiontemplatesController.php.	2021-06-28	4.3	CVE-2020-22607 CONFIRM
machform -- machform	Machform prior to version 16 is vulnerable to stored cross-site scripting due to insufficient sanitization of file attachments uploaded with forms through upload.php.	2021-06-29	4.3	CVE-2021-20103 MISC
machform -- machform	Machform prior to version 16 is vulnerable to an open redirect in Safari_init.php due to an improperly sanitized 'ref' parameter.	2021-06-29	5.8	CVE-2021-20105 MISC
machform -- machform	Machform prior to version 16 is vulnerable to HTTP host header injection due to improperly validated host headers. This could cause a victim to receive malformed content.	2021-06-29	5.8	CVE-2021-20101 MISC
machform -- machform	Machform prior to version 16 is vulnerable to cross-site request forgery due to a lack of CSRF tokens in place.	2021-06-29	6.8	CVE-2021-20102 MISC
machform -- machform	Machform prior to version 16 is vulnerable to unauthenticated remote code execution due to insufficient sanitization of file attachments uploaded with forms through upload.php.	2021-06-29	6.8	CVE-2021-20104 MISC
magento -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by an Improper Authorization vulnerability via the 'Create Customer' endpoint. Successful exploitation could lead to unauthorized modification of customer data by an unauthenticated attacker. Access to the admin console is required for successful exploitation.	2021-06-28	6.4	CVE-2021-28563 MISC
mermaid_project -- mermaid	Mermaid before 8.11.0 allows XSS when the antiscript feature is used.	2021-06-27	4.3	CVE-2021-35513 MISC MISC MISC
miniaudio_project -- miniaudio	Miniaudio 0.10.35 has an integer-based buffer overflow caused by an out-of-bounds left shift in drwav_bytes_to_u32 in miniaudio.h	2021-06-25	6.8	CVE-2021-34185 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
miraheze -- globalnewfiles	GlobalNewFiles is a mediawiki extension. All existing versions of GlobalNewFiles are affected by an uncontrolled resource consumption vulnerability. A large amount of page moves within a short space of time could overwhelm Database servers due to improper handling of load balancing and a lack of an appropriate index. No patches are currently available. As a workaround, one may avoid use of the extension unless additional rate limit at the MediaWiki level or via PoolCounter / MySQL is enabled.	2021-06-28	4	CVE-2021-32722 CONFIRM MISC
nvidia -- geforce_experience	NVIDIA GeForce Experience, all versions prior to 3.23, contains a vulnerability where, if a user clicks on a maliciously formatted link that opens the GeForce Experience login page in a new browser tab instead of the GeForce Experience application and enters their login information, the malicious site can get access to the token of the user login session. Such an attack may lead to these targeted users' data being accessed, altered, or lost.	2021-06-25	6.8	CVE-2021-1073 CONFIRM
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13679.	2021-06-29	6.8	CVE-2021-31514 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12653.	2021-06-29	6.8	CVE-2021-31507 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13674.	2021-06-29	4.3	CVE-2021-31506 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13306.	2021-06-29	6.8	CVE-2021-31508 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13678.	2021-06-29	6.8	CVE-2021-31513 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13677.	2021-06-29	6.8	CVE-2021-31512 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13309.	2021-06-29	6.8	CVE-2021-31509 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13675.	2021-06-29	6.8	CVE-2021-31510 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13676.	2021-06-29	6.8	CVE-2021-31511 MISC
oracle -- glassfish_server	** UNSUPPORTED WHEN ASSIGNED ** Oracle GlassFish Server 3.1.2.18 and below allows /common/logViewer/logViewer.jsf XSS. A malicious user can cause an administrator user to supply dangerous content to the vulnerable page, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-06-25	4.3	CVE-2021-3314 MISC MISC
phoenixcontact -- config	Phoenix Contact Classic Automation Worx Software Suite in Version 1.87 and below is affected by a remote code execution vulnerability. Manipulated PC Worx or Config+ projects could lead to a remote code execution when unallocated memory is freed because of incompletely initialized data. The attacker needs to get access to an original bus configuration file (*.bcp) to be able to manipulate data inside. After manipulation the attacker needs to exchange the original file by the manipulated one on the application programming workstation. Availability, integrity, or confidentiality of an application programming workstation might be compromised by attacks using these vulnerabilities. Automated systems in operation which were programmed with one of the above-mentioned products are not affected.	2021-06-25	5.1	CVE-2021-33542 CONFIRM
phoenixcontact -- fl_comserver_uni_232\/422\/485_firmware	In Phoenix Contact FL COMSERVER UNI in versions < 2.40 a invalid Modbus exception response can lead to a temporary denial of service.	2021-06-25	5	CVE-2021-21002 CONFIRM
phoenixcontact -- fl_switch_smcs_16tx_firmware	In Phoenix Contact FL SWITCH SMCS series products in multiple versions fragmented TCP-Packets may cause a Denial of Service of Web-, SNMP- and ICMP-Echo services. The switching functionality of the device is not affected.	2021-06-25	5	CVE-2021-21003 CONFIRM
phoenixcontact -- fl_switch_smcs_16tx_firmware	In Phoenix Contact FL SWITCH SMCS series products in multiple versions an attacker may insert malicious code via LLDP frames into the web-based management which could then be executed by the client.	2021-06-25	4.3	CVE-2021-21004 CONFIRM
postsrsd_project -- postsrsd	PostSRSd before 1.11 allows a denial of service (subprocess hang) if Postfix sends certain long data fields such as multiple concatenated email addresses. NOTE: the PostSRSd maintainer acknowledges "theoretically, this error should never occur ... I'm not sure if there's a reliable way to trigger this condition by an external attacker, but it is a security bug in PostSRSd nevertheless."	2021-06-28	5	CVE-2021-35525 MISC MISC MISC
poweriso -- poweriso	A memory corruption vulnerability exists in the DMG File Format Handler functionality of PowerISO 7.9. A specially crafted DMG file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability. The vendor fixed it in a bug-release of the current version.	2021-06-29	6.8	CVE-2021-21871 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prismjs -- prism	Prism is a syntax highlighting library. Some languages before 1.24.0 are vulnerable to Regular Expression Denial of Service (ReDoS). When Prism is used to highlight untrusted (user-given) text, an attacker can craft a string that will take a very very long time to highlight. This problem has been fixed in Prism v1.24. As a workaround, do not use ASCIIDoc or ERB to highlight untrusted text. Other languages are not affected and can be used to highlight untrusted text.	2021-06-28	4.3	CVE-2021-32723 CONFIRM MISC MISC
python -- urllib3	An issue was discovered in urllib3 before 1.26.5. When provided with a URL containing many @ characters in the authority component, the authority regular expression exhibits catastrophic backtracking, causing a denial of service if a URL were passed as a parameter or redirected to via an HTTP redirect.	2021-06-29	5	CVE-2021-33503 CONFIRM CONFIRM
shopex -- ecshop	Cross Site Scripting (XSS) vulnerability in ECShop 4.0 due to security filtering issues, in the user.php file, we can use the html entity encoding to bypass the security policy of the safety.php file, triggering the xss vulnerability.	2021-06-28	4.3	CVE-2020-20640 MISC
siemens -- sinamics_sl150_firmware	The Telnet service of the SIMATIC HMI Comfort Panels system component in affected products does not require authentication, which may allow a remote attacker to gain access to the device if the service is enabled. Telnet is disabled by default on the SINAMICS Medium Voltage Products (SINAMICS SL150: All versions, SINAMICS SM150: All versions, SINAMICS SM150i: All versions).	2021-06-28	6.8	CVE-2021-31337 MISC
sylius -- sylius	Sylius is an Open Source eCommerce platform on top of Symfony. In versions of Sylius prior to 1.9.5 and 1.10.0-RC.1, part of the details (order ID, order number, items total, and token value) of all placed orders were exposed to unauthorized users. If exploited properly, a few additional information like the number of items in the cart and the date of the shipping may be fetched as well. This data seems to not be crucial nor is personal data, however, could be used for sociotechnical attacks or may expose a few details about shop condition to the third parties. The data possible to aggregate are the number of processed orders or their value in the moment of time. The problem has been patched at Sylius 1.9.5 and 1.10.0-RC.1. There are a few workarounds for the vulnerability. The first possible solution is to hide the problematic endpoints behind the firewall from not logged in users. This would put only the order list under the firewall and allow only authorized users to access it. Once a user is authorized, it will have access to theirs orders only. The second possible solution is to decorate the `\Sylius\Bundle\ApiBundle\Doctrine\QueryCollectionExtension\OrdersByLoggedInUserExtension` and throw `Symfony\Component\Security\Core\Exception\AccessDeniedException` if the class is executed for unauthorized user.	2021-06-28	5	CVE-2021-32720 CONFIRM MISC
tenable -- nessus	Nessus Agent 8.2.4 and earlier for Windows were found to contain multiple local privilege escalation vulnerabilities which could allow an authenticated, local administrator to run specific Windows executables as the Nessus host. This is different than CVE-2021-20099.	2021-06-28	4.6	CVE-2021-20100 MISC
tenable -- nessus	Nessus Agent 8.2.4 and earlier for Windows were found to contain multiple local privilege escalation vulnerabilities which could allow an authenticated, local administrator to run specific Windows executables as the Nessus host. This is different than CVE-2021-20100.	2021-06-28	4.6	CVE-2021-20099 MISC
umbraco -- umbraco_cms	Umbraco CMS before 7.15.7 is vulnerable to Open Redirection due to insufficient url sanitization on booting.aspx.	2021-06-28	5.8	CVE-2021-34254 MISC
unidocs -- ezpdf_editor	A memory corruption vulnerability exists when ezPDF improperly handles the parameter. This vulnerability exists due to insufficient validation of the parameter.	2021-06-29	6.5	CVE-2020-7870 MISC
vector35 -- binary_ninja	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Vector 35 Binary Ninja 2.3.2660 (Build ID 88f343c3). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BNDB files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13670.	2021-06-29	6.8	CVE-2021-31516 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vector35 -- binary_ninja	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Vector 35 Binary Ninja 2.3.2660 (Build ID 88f343c3). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BNDB files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13668.	2021-06-29	6.8	CVE-2021-31515 MISC MISC
vmware -- spring_security	Spring Security versions 5.5.x prior to 5.5.1, 5.4.x prior to 5.4.7, 5.3.x prior to 5.3.10 and 5.2.x prior to 5.2.11 are susceptible to a Denial-of-Service (DoS) attack via the initiation of the Authorization Request in an OAuth 2.0 Client Web and WebFlux application. A malicious user or attacker can send multiple requests initiating the Authorization Request for the Authorization Code Grant, which has the potential of exhausting system resources using a single session or multiple sessions.	2021-06-29	5	CVE-2021-22119 MISC
webport_cms_project -- webport_cms	Directory Traversal vulnerability in Webport CMS 1.19.10.17121 via the file parameter to file/download.	2021-06-28	5	CVE-2020-23715 MISC
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable denial-of-service vulnerability exists in ServiceAgent functionality. A specially crafted packet can cause an integer underflow, triggering a large memcpy that will access unmapped or out-of-bounds memory. An attacker can send this packet while unauthenticated to trigger this vulnerability.	2021-06-25	5	CVE-2021-33536 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable format string vulnerability exists in the iw_console conio_writestr functionality. A specially crafted time server entry can cause an overflow of the time server buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	6.5	CVE-2021-33535 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions the usage of hard-coded cryptographic keys within the service agent binary allows for the decryption of captured traffic across the network from or to the device.	2021-06-25	5	CVE-2021-33529 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable authentication bypass vulnerability exists in the hostname processing. A specially configured device hostname can cause the device to interpret selected remote traffic as local traffic, resulting in a bypass of web authentication. An attacker can send authenticated SNMP requests to trigger this vulnerability.	2021-06-25	6.5	CVE-2021-33539 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable remote code execution vulnerability exists in the iw_webs configuration parsing functionality. A specially crafted user name entry can cause an overflow of an error message buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	6.5	CVE-2021-33537 CONFIRM
zammad -- zammad	Cross Site Scripting (XSS) in Zammad 1.0.x up to 4.0.0 allows remote attackers to execute arbitrary web script or HTML via multiple models that contain a 'note' field to store additional information.	2021-06-28	4.3	CVE-2021-35298 CONFIRM
zammad -- zammad	Text injection/Content Spoofing in 404 page in Zammad 1.0.x up to 4.0.0 could allow remote attackers to manipulate users into visiting the attackers' page.	2021-06-28	4.3	CVE-2021-35300 CONFIRM
zammad -- zammad	Cross Site Scripting (XSS) in Zammad 1.0.x up to 4.0.0 allows remote attackers to execute arbitrary web script or HTML via the User Avatar attribute.	2021-06-28	4.3	CVE-2021-35303 CONFIRM
zammad -- zammad	Incorrect Access Control for linked Tickets in Zammad 1.0.x up to 4.0.0 allows remote attackers to obtain sensitive information.	2021-06-28	5	CVE-2021-35302 CONFIRM
zammad -- zammad	Incorrect Access Control in Zammad 1.0.x up to 4.0.0 allows remote attackers to obtain sensitive information via the Ticket Article detail view.	2021-06-28	5	CVE-2021-35301 CONFIRM
zammad -- zammad	Incorrect Access Control in Zammad 1.0.x up to 4.0.0 allows attackers to obtain sensitive information via email connection configuration probing.	2021-06-28	5	CVE-2021-35299 CONFIRM
zohocorp -- manageengine_servicedesk_plus	Zoho ManageEngine ServiceDesk Plus MSP before 10521 allows an attacker to access internal data.	2021-06-29	5	CVE-2021-31160 CONFIRM MISC
zohocorp -- manageengine_servicedesk_plus_msp	Zoho ManageEngine ServiceDesk Plus MSP before 10522 is vulnerable to Information Disclosure.	2021-06-29	5	CVE-2021-31530 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zrlog -- zrlog	Cross Site Scripting vulnerability in ZrLog 2.1.0 via the (1) userName and (2) email parameters in post/addComment.	2021-06-29	4.3	CVE-2020-18066 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- photoshop_elements	Adobe Photoshop Elements version 5.2 (and earlier) is affected by an insecure temporary file creation vulnerability. An unauthenticated attacker could leverage this vulnerability to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction.	2021-06-28	2.1	CVE-2021-28597 MISC
adobe -- premiere_elements	Adobe Premiere Elements version 5.2 (and earlier) is affected by an insecure temporary file creation vulnerability. An unauthenticated attacker could leverage this vulnerability to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction.	2021-06-28	2.1	CVE-2021-28623 MISC
bluetooth -- bluetooth_core_specification	Unencrypted Bluetooth Low Energy baseband links in Bluetooth Core Specifications 4.0 through 5.2 may permit an adjacent device to inject a crafted packet during the receive window of the listening device before the transmitting device initiates its packet transmission to achieve full MITM status without terminating the link. When applied against devices establishing or using encrypted links, crafted packets may be used to terminate an existing link, but will not compromise the confidentiality or integrity of the link.	2021-06-25	2.9	CVE-2021-31615 MISC MISC
cabrerahector -- popular_posts	Cross-site scripting vulnerability in WordPress Popular Posts 5.3.2 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	2021-06-28	3.5	CVE-2021-20746 MISC MISC MISC MISC
dovecot -- dovecot	Dovecot before 2.3.15 allows ../ Path Traversal. An attacker with access to the local filesystem can trick OAuth2 authentication into using an HS256 validation key from an attacker-controlled location. This occurs during use of local JWT validation with the posix fs driver.	2021-06-28	2.1	CVE-2021-29157 MISC CONFIRM
ibm -- aix	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user that is in the with elevated group privileges to cause a denial of service due to a vulnerability in the lpd daemon. IBM X-Force ID: 200255.	2021-06-28	2.1	CVE-2021-29693 XF CONFIRM
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 could allow an authenticated user to obtain sensitive information about another user under nondefault configurations. IBM X-Force ID: 201779.	2021-06-28	3.5	CVE-2021-29751 CONFIRM CONFIRM XF
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196949.	2021-06-29	3.5	CVE-2021-20477 CONFIRM XF
ibm -- security_verify	IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2021-06-25	3.5	CVE-2021-29677 CONFIRM XF
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.8 could allow a local user to cause a denial of service due to insecure file permission settings. IBM X-Force ID: 197791.	2021-06-29	2.1	CVE-2021-20490 CONFIRM XF
limesurvey -- limesurvey	Cross Site Scripting (XSS) vulneraiblity in LimeSurvey 4.2.5 on textbox via the Notifications & data feature.	2021-06-28	3.5	CVE-2020-23710 MISC
magento -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a DOM-based Cross-Site Scripting vulnerability on mage-messages cookies. Successful exploitation could lead to arbitrary JavaScript execution by an unauthenticated attacker. User interaction is required for successful exploitation.	2021-06-28	3.5	CVE-2021-28556 MISC
pandorafms -- pandora_fms	PandoraFMS <=7.54 allows Stored XSS by placing a payload in the name field of a visual console. When a user or an administrator visits the console, the XSS payload will be executed.	2021-06-25	3.5	CVE-2021-35501 MISC
plone -- plone	In Plone 5.0 through 5.2.4, Editors are vulnerable to XSS in the folder contents view, if a Contributor has created a folder with a SCRIPT tag in the description field.	2021-06-30	3.5	CVE-2021-35959 MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sas -- environment_manager	SAS Environment Manager 2.5 allows XSS through the Name field when creating/editing a server. The XSS will prompt when editing the Configuration Properties.	2021-06-25	3.5	CVE-2021-35475 MISC MISC MISC
sick -- visionary-s_cx_firmware	SICK Visionary-S CX up version 5.21.2.29154R are vulnerable to an Inadequate Encryption Strength vulnerability concerning the internal SSH interface solely used by SICK for recovering returned devices. The use of weak ciphers make it easier for an attacker to break the security that protects information transmitted from the client to the SSH server, assuming the attacker has access to the network on which the device is connected. This can increase the risk that encryption will be compromised, leading to the exposure of sensitive user information and man-in-the-middle attacks.	2021-06-28	3.5	CVE-2021-32496 MISC
tripplite -- su2200rtxl2ua_firmware	A stored cross-site scripting (XSS) vulnerability was discovered in /Forms/device_vars_1 on TrippLite SU2200RTXL2Ua with firmware version 12.04.0055. This vulnerability allows authenticated attackers to obtain other users' information via a crafted POST request.	2021-06-25	3.5	CVE-2020-26801 MISC MISC MISC
vmware -- rabbitmq	RabbitMQ is a multi-protocol messaging broker. In rabbitmq-server prior to version 3.8.17, a new user being added via management UI could lead to the user's bane being rendered in a confirmation message without proper `<script>` tag sanitization, potentially allowing for JavaScript code execution in the context of the page. In order for this to occur, the user must be signed in and have elevated permissions (other user management). The vulnerability is patched in RabbitMQ 3.8.17. As a workaround, disable `rabbitmq_management` plugin and use CLI tools for management operations and Prometheus and Grafana for metrics and monitoring.	2021-06-28	3.5	CVE-2021-32718 CONFIRM MISC
vmware -- rabbitmq	RabbitMQ is a multi-protocol messaging broker. In rabbitmq-server prior to version 3.8.18, when a federation link was displayed in the RabbitMQ management UI via the `rabbitmq_federation_management` plugin, its consumer tag was rendered without proper <script> tag sanitization. This potentially allows for JavaScript code execution in the context of the page. The user must be signed in and have elevated permissions (manage federation upstreams and policies) for this to occur. The vulnerability is patched in RabbitMQ 3.8.18. As a workaround, disable the `rabbitmq_federation_management` plugin and use [CLI tools](https://www.rabbitmq.com/cli.html) instead.	2021-06-28	3.5	CVE-2021-32719 MISC CONFIRM MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_reader_dc	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by a Use After Free vulnerability when executing search queries through Javascript. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-28562 MISC
adobe -- animate	Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-28575 MISC
adobe -- animate	Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-28574 MISC
adobe -- animate	Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-28576 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Adobe Illustrator version 25.2 (and earlier) is affected by a Path Traversal vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-21102 MISC
adobe -- illustrator	Adobe Illustrator version 25.2 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-21101 MISC
adobe -- incopy	Adobe InCopy version 16.0 (and earlier) is affected by an path traversal vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-21090 MISC
adobe -- indesign	Adobe InDesign version 16.0 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-21099 MISC
adobe -- indesign	Adobe InDesign version 16.0 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	not yet calculated	CVE-2021-21098 MISC
adobe -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a Violation of Secure Design Principles vulnerability in RMA PDF filename formats. Successful exploitation could allow an attacker to get unauthorized access to restricted resources.	2021-06-28	not yet calculated	CVE-2021-28583 MISC
adobe -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a Path Traversal vulnerability when creating a store with child theme.Successful exploitation could lead to arbitrary file system write by an authenticated attacker. Access to the admin console is required for successful exploitation.	2021-06-28	not yet calculated	CVE-2021-28584 MISC
adobe -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by an Improper input validation vulnerability in the New customer WebAPI.Successful exploitation could allow an attacker to send unsolicited spam e-mails.	2021-06-28	not yet calculated	CVE-2021-28585 MISC
akcp -- akcp	Stored cross-site scripting (XSS) in the embedded webserver of AKCP sensorProbe before SP480-20210624 enables remote authenticated attackers to introduce arbitrary JavaScript via the Sensor Description, Email (from/to/cc), System Name, and System Location fields.	2021-06-30	not yet calculated	CVE-2021-35956 MISC MISC MISC
akkadian -- provisioning_manager	An issue exists within Akkadian Provisioning Manager 4.50.02 which allows attackers to view sensitive information within the /pme subdirectories.	2021-07-01	not yet calculated	CVE-2020-27361 MISC
akkadian -- provisioning_manager	An issue exists within the SSH console of Akkadian Provisioning Manager 4.50.02 which allows a low-level privileged user to escape the web configuration file editor and escalate privileges.	2021-07-01	not yet calculated	CVE-2020-27362 MISC
apache -- druid	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource.	2021-07-02	not yet calculated	CVE-2021-26920 MISC MLIST
apache -- traffic_server	Incorrect handling of url fragment vulnerability of Apache Traffic Server allows an attacker to poison the cache. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-29	not yet calculated	CVE-2021-27577 MISC
apache -- traffic_server	Invalid values in the Content-Length header sent to Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-29	not yet calculated	CVE-2021-32565 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- traffic_server	Stack-based Buffer Overflow vulnerability in cachekey plugin of Apache Traffic Server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-30	not yet calculated	CVE-2021-35474 MISC
arlo_q_plus -- arlo_q_plus	This vulnerability allows attackers with physical access to escalate privileges on affected installations of Arlo Q Plus 1.9.0.3_278. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSH service. The device can be booted into a special operation mode where hard-coded credentials are accepted for SSH authentication. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-12890.	2021-06-29	not yet calculated	CVE-2021-31505 MISC MISC
artica -- pandora_fms	In Artica Pandora FMS <=754 in the File Manager component, there is sensitive information exposed on the client side which attackers can access.	2021-06-30	not yet calculated	CVE-2021-34075 MISC
chevereto -- chevereto	Chevereto before 3.17.1 allows Cross Site Scripting (XSS) via an image title at the image upload stage.	2021-06-30	not yet calculated	CVE-2021-31721 MISC MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Search Text" field under the "Admin Search" module.	2021-07-02	not yet calculated	CVE-2020-36412 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Path for the {page_image} tag:" or "Path for thumbnail field:" parameters under the "Content Editing Settings" module.	2021-07-02	not yet calculated	CVE-2020-36411 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Email address to receive notification of news submission" parameter under the "Options" module.	2021-07-02	not yet calculated	CVE-2020-36410 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "URL (slug)" or "Extra" fields under the "Add Article" feature.	2021-07-02	not yet calculated	CVE-2020-36414 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add Shortcut" parameter under the "Manage Shortcuts" module.	2021-07-02	not yet calculated	CVE-2020-36408 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Exclude these IP addresses from the "Site Down" status" parameter under the "Maintenance Mode" module.	2021-07-02	not yet calculated	CVE-2020-36413 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Create a new Stylesheet" parameter under the "Stylesheets" module.	2021-07-02	not yet calculated	CVE-2020-36415 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Create a new Design" parameter under the "Designs" module.	2021-07-02	not yet calculated	CVE-2020-36416 MISC
cms_made_simple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add Category" parameter under the "Categories" module.	2021-07-02	not yet calculated	CVE-2020-36409 MISC
coral -- coral	Talk 4 in Coral before 4.12.1 allows remote attackers to discover e-mail addresses and other sensitive information via GraphQL because permission checks use an incorrect data type.	2021-06-30	not yet calculated	CVE-2021-35970 MISC MISC MISC MISC
craft_cms -- craft_cms	An issue was discovered in Craft CMS before 3.6.7. In some circumstances, a potential Remote Code Execution vulnerability existed on sites that did not restrict administrative changes (if an attacker were somehow able to hijack an administrator's session).	2021-06-30	not yet calculated	CVE-2021-27903 MISC MISC MISC
craft_cms -- craft_cms	An issue was discovered in Craft CMS before 3.6.0. In some circumstances, a potential XSS vulnerability existed in connection with front-end forms that accepted user uploads.	2021-06-30	not yet calculated	CVE-2021-27902 MISC MISC MISC
delta_electronics -- dopsoft	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to disclose information.	2021-07-02	not yet calculated	CVE-2021-27455 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
delta_electronics -- dopsoft	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	2021-07-02	not yet calculated	CVE-2021-27412 MISC
django -- django	Django 3.1.x before 3.1.13 and 3.2.x before 3.2.5 allows QuerySet.order_by SQL injection if order_by is untrusted input from a client of a web application.	2021-07-02	not yet calculated	CVE-2021-35042 MISC CONFIRM MISC CONFIRM
djvulibre -- djvulibre	An out-of-bounds write vulnerability was found in DjVuLibre in DJVU::DjVuTXT::decode() in DjVuText.cpp via a crafted djvu file which may lead to crash and segmentation fault. This flaw affects DjVuLibre versions prior to 3.5.28.	2021-06-30	not yet calculated	CVE-2021-3630 MISC
ec-cube -- ec-cube	Improper access control vulnerability in EC-CUBE 4.0.6 (EC-CUBE 4 series) allows a remote attacker to bypass access restriction and obtain sensitive information via unspecified vectors.	2021-07-01	not yet calculated	CVE-2021-20778 MISC MISC JVN
ec-cube -- ec-cube	Cross-site scripting vulnerability in EC-CUBE EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.	2021-06-28	not yet calculated	CVE-2021-20751 MISC MISC
ec-cube -- ec-cube	Cross-site scripting vulnerability in EC-CUBE EC-CUBE 3.0.0 to 3.0.18-p2 (EC-CUBE 3 series) and EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.	2021-06-28	not yet calculated	CVE-2021-20750 MISC MISC MISC
emissary -- emissary	Emissary is a P2P-based, data-driven workflow engine. Emissary version 6.4.0 is vulnerable to Server-Side Request Forgery (SSRF). In particular, the `RegisterPeerAction` endpoint and the `AddChildDirectoryAction` endpoint are vulnerable to SSRF. This vulnerability may lead to credential leaks. Emissary version 7.0 contains a patch. As a workaround, disable network access to Emissary from untrusted sources.	2021-07-02	not yet calculated	CVE-2021-32639 CONFIRM MISC MISC
ethereum -- solidity	Solidity 0.7.5 has a stack-use-after-return issue in smtutil::CHCSmtLib2Interface::querySolver. NOTE: c39a5e2b7a3fabbf687f53a2823fc087be6c1a7e is cited in the OSV "fixed" field but does not have a code change.	2021-07-01	not yet calculated	CVE-2020-36402 MISC MISC MISC
fluent -- fluent_bit	Fluent Bit (aka fluent-bit) 1.7.0 through 1.7,4 has a double free in flb_free (called from flb_parser_json_do and flb_parser_do).	2021-07-01	not yet calculated	CVE-2021-36088 MISC MISC MISC MISC
fudousan_plugin_pro -- fudousan_plugin_pro	Cross-site scripting vulnerability in Fudousan plugin ver5.7.0 and earlier, Fudousan Plugin Pro Single-User Type ver5.7.0 and earlier, and Fudousan Plugin Pro Multi-User Type ver5.7.0 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	2021-06-28	not yet calculated	CVE-2021-20749 MISC MISC MISC
getkirby -- kirby	Kirby is a content management system. In Kirby CMS versions 3.5.5 and 3.5.6, the Panel's `ListItem` component (used in the pages and files section for example) displayed HTML in page titles as it is. This could be used for cross-site scripting (XSS) attacks. Malicious authenticated Panel users can escalate their privileges if they get access to the Panel session of an admin user. Visitors without Panel access can use the attack vector if the site allows changing site data from a frontend form. Kirby 3.5.7 patches the vulnerability. As a partial workaround, site administrators can protect against attacks from visitors without Panel access by validating or sanitizing provided data from the frontend form.	2021-07-02	not yet calculated	CVE-2021-32735 CONFIRM MISC
google -- chrome	Use after free in WebGL in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-07-02	not yet calculated	CVE-2021-30554 MISC MISC
google -- chrome	Use after free in Sharing in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and user gesture.	2021-07-02	not yet calculated	CVE-2021-30555 MISC MISC
google -- chrome	Use after free in WebAudio in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-07-02	not yet calculated	CVE-2021-30556 MISC MISC
google -- chrome	Use after free in TabGroups in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-07-02	not yet calculated	CVE-2021-30557 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
grok -- grok	Grok 7.6.6 through 9.2.0 has a heap-based buffer overflow in grk::FileFormatDecompress::apply_palette_clr (called from grk::FileFormatDecompress::applyColour).	2021-07-01	not yet calculated	CVE-2021-36089 MISC MISC MISC
hitachi -- virtual_file_platform_versions	Hitachi Virtual File Platform Versions prior to 5.5.3-09 and Versions prior to 6.4.3-09, and NEC Storage M Series NAS Gateway Nh4a/Nh8a versions prior to FOS 5.5.3-08(NEC2.5.4a) and Nh4b/Nh8b, Nh4c/Nh8c versions prior to FOS 6.4.3-08(NEC3.4.2) allow remote authenticated attackers to execute arbitrary OS commands with root privileges via unspecified vectors.	2021-06-28	not yet calculated	CVE-2021-20740 MISC MISC MISC
huawei -- multiple_products	There is a multiple threads race condition vulnerability in Huawei product. A race condition exists for concurrent I/O read by multiple threads. An attacker with the root permission can exploit this vulnerability by performing some operations. Successful exploitation of this vulnerability may cause the system to crash. Affected product versions include: ManageOne 6.5.1.SPC200, 8.0.0,8.0.0-LCND81, 8.0.0.SPC100, 8.0.1,8.0.RC2, 8.0.RC3, 8.0.RC3.SPC100;SMC2.0 V600R019C10SPC700,V600R019C10SPC702, V600R019C10SPC703,V600R019C10SPC800, V600R019C10SPC900, V600R019C10SPC910, V600R019C10SPC920, V600R019C10SPC921, V600R019C10SPC922, V600R019C10SPC930, V600R019C10SPC931	2021-06-29	not yet calculated	CVE-2021-22340 MISC
huawei -- multiple_products	There has a license management vulnerability in some Huawei products. An attacker with high privilege needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper license management of the device, as a result, the license file can be applied and affect integrity of the device. Affected product versions include:S12700 V200R007C01,V200R007C01B102,V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S2700 V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S5700 V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10,V200R011C10SPC100;S V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10,V200R011C10SPC100;S V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S9700 V200R007C01,V200R007C01B102,V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V2C	2021-06-29	not yet calculated	CVE-2021-22329 MISC
huawei -- smartphone	There is an Improper Validation of Array Index Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause stability risks.	2021-06-30	not yet calculated	CVE-2021-22374 MISC
huawei -- smartphone	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause the device to crash and restart.	2021-06-30	not yet calculated	CVE-2021-22350 MISC
huawei -- smartphone	There is a Credentials Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may induce users to grant permissions on modifying items in the configuration table,causing system exceptions.	2021-06-30	not yet calculated	CVE-2021-22351 MISC
huawei -- smartphone	There is a Configuration Defect Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may allow attackers to hijack the device and forge UIs to induce users to execute malicious commands.	2021-06-30	not yet calculated	CVE-2021-22352 MISC
huawei -- smartphone	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause the kernel to restart.	2021-06-30	not yet calculated	CVE-2021-22353 MISC
huawei -- smartphone	There is a Key Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may lead to authentication bypass.	2021-06-30	not yet calculated	CVE-2021-22367 MISC
huawei -- smartphone	There is a Permission Control Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect normal use of the device.	2021-06-30	not yet calculated	CVE-2021-22368 MISC
huawei -- smartphone	There is an Input Verification Vulnerability in Huawei Smartphone. Successful exploitation of insufficient input verification may cause the system to restart.	2021-06-30	not yet calculated	CVE-2021-22349 MISC
huawei -- smartphone	There is a Defects Introduced in the Design Process Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service integrity and availability.	2021-06-30	not yet calculated	CVE-2021-22373 MISC
huawei -- smartphone	There is an Improper Permission Management Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	2021-06-30	not yet calculated	CVE-2021-22371 MISC
huawei -- smartphone	There is a Security Features Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	2021-06-30	not yet calculated	CVE-2021-22372 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- smartphone	There is a Key Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality,availability and integrity.	2021-06-30	not yet calculated	CVE-2021-22375 MISC
huawei -- smartphone	There is an Improper Permission Management Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality, availability and integrity.	2021-06-30	not yet calculated	CVE-2021-22376 MISC
huawei -- smartphone	There is a Cleartext Transmission of Sensitive Information Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality and availability.	2021-06-30	not yet calculated	CVE-2021-22380 MISC
huawei -- smartphone	There is a Credentials Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	2021-06-30	not yet calculated	CVE-2021-22370 MISC
huawei -- smartphone	There is a Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability in Huawei Smartphone. Successful exploitation of these vulnerabilities may escalate the permission to that of the root user.	2021-06-30	not yet calculated	CVE-2021-22369 MISC
huawei -- smartphone	There is a Configuration Defect vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service integrity and availability.	2021-07-01	not yet calculated	CVE-2021-22343 MISC
huawei -- smartphone	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS.	2021-07-01	not yet calculated	CVE-2021-22344 MISC
huawei -- smartphone	There is a Missing Cryptographic Step vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause DoS of Samgr.	2021-07-01	not yet calculated	CVE-2020-9158 MISC
huawei -- smartphone	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause code to execute.	2021-06-30	not yet calculated	CVE-2021-22348 MISC
huawei -- smartphone	There is an Improper Permission Management Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may lead to the disclosure of user habits.	2021-06-30	not yet calculated	CVE-2021-22346 MISC
huawei -- smartphone	There is an Input Verification Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause out-of-bounds memory write.	2021-06-30	not yet calculated	CVE-2021-22345 MISC
huawei -- smartphone	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS.	2021-07-01	not yet calculated	CVE-2021-22347 MISC
huawei -- smartphone	There is an Incorrect Privilege Assignment Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	2021-06-30	not yet calculated	CVE-2021-22326 MISC
huawei -- smartphone	There is an Integer Overflow Vulnerability in Huawei Smartphone. Successful exploitation of these vulnerabilities may escalate the permission to that of the root user.	2021-06-30	not yet calculated	CVE-2021-22323 MISC
ibm -- cognos_analytics	IBM Cognos Analytics 10.0 and 11.1 is susceptible to a weakness in the implementation of the System Appearance configuration setting. An attacker could potentially bypass business logic to modify the appearance and behavior of the application. IBM X-Force ID: 196770.	2021-06-30	not yet calculated	CVE-2021-20461 XF CONFIRM
ibm -- datacap_fastdoc_capture	IBM Datacap Fastdoc Capture (IBM Datacap Navigator 9.1.7) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 191753.	2021-07-01	not yet calculated	CVE-2020-4935 CONFIRM XF
ibm -- datacap_taskmaster_capture	IBM Datacap Taskmaster Capture (IBM Datacap Navigator 9.1.7) is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 191045.	2021-07-01	not yet calculated	CVE-2020-4902 XF CONFIRM
ibm -- security_identity_manager_adapters	IBM Security Identity Manager Adapters 6.0 and 7.0 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability and takeover other accounts. IBM X-Force ID: 199252.	2021-06-28	not yet calculated	CVE-2021-20574 CONFIRM XF
jenkins -- jenkins	A missing permission check in Jenkins requests-plugin Plugin 2.2.6 and earlier allows attackers with Overall/Read permission to view the list of pending requests.	2021-06-30	not yet calculated	CVE-2021-21674 CONFIRM MLIST
jenkins -- jenkins	Jenkins requests-plugin Plugin 2.2.7 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to send test emails to an attacker-specified email address.	2021-06-30	not yet calculated	CVE-2021-21676 CONFIRM MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins CAS Plugin 1.6.0 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins, allowing attackers to perform phishing attacks.	2021-06-30	not yet calculated	CVE-2021-21673 CONFIRM MLIST
jenkins -- jenkins	Jenkins Selenium HTML report Plugin 1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2021-06-30	not yet calculated	CVE-2021-21672 CONFIRM MLIST
jenkins -- jenkins	Jenkins 2.299 and earlier, LTS 2.289.1 and earlier does not invalidate the previous session on login.	2021-06-30	not yet calculated	CVE-2021-21671 CONFIRM MLIST
jenkins -- jenkins	Jenkins 2.299 and earlier, LTS 2.289.1 and earlier allows users to cancel queue items and abort builds of jobs for which they have Item/Cancel permission even when they do not have Item/Read permission.	2021-06-30	not yet calculated	CVE-2021-21670 CONFIRM MLIST
jenkins -- jenkins	A cross-site request forgery (CSRF) vulnerability in Jenkins requests-plugin Plugin 2.2.12 and earlier allows attackers to create requests and/or have administrators apply pending requests.	2021-06-30	not yet calculated	CVE-2021-21675 CONFIRM MLIST
johnson_controls -- c-cure_9000	An insecure client auto update feature in C-CURE 9000 can allow remote execution of lower privileged Windows programs.	2021-07-01	not yet calculated	CVE-2021-27660 CERT CONFIRM
johnson_controls -- facility_explorer	Successful exploitation of this vulnerability could give an authenticated Facility Explorer SNC Series Supervisory Controller (F4-SNC) user an unintended level of access to the controller's file system, allowing them to access or modify system files by sending specifically crafted web messages to the F4-SNC.	2021-07-01	not yet calculated	CVE-2021-27661 CERT CONFIRM
jtekt_corporation -- toyopuc_plc	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop.	2021-07-01	not yet calculated	CVE-2021-27477 MISC
kde -- kimageformats	KDE KImageFormats 5.70.0 through 5.81.0 has a stack-based buffer overflow in XCFImageFormat::loadTileRLE.	2021-07-01	not yet calculated	CVE-2021-36083 MISC MISC MISC
keystone_engine -- keystone_engine	Keystone Engine 0.9.2 has a use-after-free in llvm_ks::X86Operand::getToken.	2021-07-01	not yet calculated	CVE-2020-36405 MISC MISC MISC
keystone_engine -- keystone_engine	Keystone Engine 0.9.2 has an invalid free in llvm_ks::SmallVectorImpl<llvm_ks::MCFixup>::~SmallVectorImpl.	2021-07-01	not yet calculated	CVE-2020-36404 MISC MISC MISC
lavalite -- cms	A stored cross site scripting (XSS) vulnerability in the /admin/user/team component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	2021-07-02	not yet calculated	CVE-2020-36395 MISC
lavalite -- cms	A stored cross site scripting (XSS) vulnerability in the /admin/roles/role component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	2021-07-02	not yet calculated	CVE-2020-36396 MISC
lavalite -- cms	A stored cross site scripting (XSS) vulnerability in the /admin/contact/contact component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	2021-07-02	not yet calculated	CVE-2020-36397 MISC
libavif -- libavif	libavif 0.8.0 and 0.8.1 has an out-of-bounds write in avifDecoderDataFillImageGrid.	2021-07-01	not yet calculated	CVE-2020-36407 MISC MISC MISC
libredgw -- libredwg	GNU LibreDWG 0.12.3.4163 through 0.12.3.4191 has a double-free in bit_chain_free (called from dwg_encode_MTEXT and dwg_encode_add_object).	2021-07-01	not yet calculated	CVE-2021-36080 MISC MISC MISC
libressl -- libressl	LibreSSL 2.9.1 through 3.2.1 has a heap-based buffer over-read in do_print_ex (called from asn1_item_print_ctx and ASN1_item_print).	2021-07-01	not yet calculated	CVE-2019-25048 MISC MISC MISC
libressl -- libressl	LibreSSL 2.9.1 through 3.2.1 has an out-of-bounds read in asn1_item_print_ctx (called from asn1_template_print_ctx).	2021-07-01	not yet calculated	CVE-2019-25049 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lkalka_rss_reader -- lkalka_rss_reader	Cross-site scripting vulnerability in Ikalka RSS Reader all versions allows a remote attacker to inject an arbitrary script via unspecified vectors.	2021-07-01	not yet calculated	CVE-2021-20752 MISC
mediawiki -- mediawiki	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalUserRights page provided search results which, for a suppressed MediaWiki user, were different than for any other user, thus easily disclosing suppressed accounts (which are supposed to be completely hidden).	2021-07-02	not yet calculated	CVE-2021-36127 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalRenameRequest page is vulnerable to infinite loops and denial of service attacks when a user's current username is beyond an arbitrary maximum configuration value (MaxNameChars).	2021-07-02	not yet calculated	CVE-2021-36125 MISC MISC
mediawiki -- mediawiki	An XSS issue was discovered in the SportsTeams extension in MediaWiki through 1.36. Within several special pages, a privileged user could inject arbitrary HTML and JavaScript within various data fields. The attack could easily propagate across many pages for many users.	2021-07-02	not yet calculated	CVE-2021-36131 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension in MediaWiki through 1.36. If the MediaWiki:Abusefilter-blocker message is invalid within the content language, the filter user falls back to the English version, but that English version could also be invalid on a wiki. This would result in a fatal error, and potentially fail to block or restrict a potentially nefarious user.	2021-07-02	not yet calculated	CVE-2021-36126 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the FileImporter extension in MediaWiki through 1.36. For certain relaxed configurations of the $wgFileImporterRequiredRight variable, it might not validate all appropriate user rights, thus allowing a user with insufficient rights to perform operations (specifically file uploads) that they should not be allowed to perform.	2021-07-02	not yet calculated	CVE-2021-36132 MISC MISC
mediawiki -- mediawiki	An XSS issue was discovered in the SocialProfile extension in MediaWiki through 1.36. Within several gift-related special pages, a privileged user with the awardmanage right could inject arbitrary HTML and JavaScript within various gift-related data fields. The attack could easily propagate across many pages for many users.	2021-07-02	not yet calculated	CVE-2021-36130 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. Autoblocks for CentralAuth-issued suppression blocks are not properly implemented.	2021-07-02	not yet calculated	CVE-2021-36128 MISC MISC MISC
mediawiki -- mediawiki	In MediaWiki before 1.31.15, 1.32.x through 1.35.x before 1.35.3, and 1.36.x before 1.36.1, bots have certain unintended API access. When a bot account has a "sitewide block" applied, it is able to still "purge" pages through the MediaWiki Action API (which a "sitewide block" should have prevented).	2021-07-02	not yet calculated	CVE-2021-35197 CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the Translate extension in MediaWiki through 1.36. The Aggregategroups Action API module does not validate the parameter for aggregategroup when action=remove is set, thus allowing users with the translate-manage right to silently delete various groups' metadata.	2021-07-02	not yet calculated	CVE-2021-36129 MISC MISC
microsoft -- windows	Windows Print Spooler Remote Code Execution Vulnerability	2021-07-02	not yet calculated	CVE-2021-34527 MISC
monstra_cms -- monstra	Monstra CMS 3.0.4 allows attackers to execute arbitrary code via a crafted payload entered into the "Snippet content" field under the "Edit Snippet" module.	2021-07-01	not yet calculated	CVE-2020-23219 MISC
monstra_cms -- monstra	A stored cross site scripting (XSS) vulnerability in Monstra CMS version 3.0.4 allows attackers to execute arbitrary web scripts or HTML via crafted a payload entered into the "Site Name" field under the "Site Settings" module.	2021-07-01	not yet calculated	CVE-2020-23205 MISC
mruby -- mruby	mruby 2.1.2 has a double free in mrb_default_allocf (called from mrb_free and obj_free).	2021-07-01	not yet calculated	CVE-2020-36401 MISC MISC MISC
netgear -- wac104_devices	NETGEAR WAC104 devices before 1.0.4.15 are affected by an authentication bypass vulnerability in /usr/sbin/mini_httpd, allowing an unauthenticated attacker to invoke any action by adding the &currentsetting.htm substring to the HTTP query, a related issue to CVE-2020-27866. This directly allows the attacker to change the web UI password, and eventually to enable debug mode (telnetd) and gain a shell on the device as the admin limited-user account (however, escalation to root is simple because of weak permissions on the /etc/ directory).	2021-06-30	not yet calculated	CVE-2021-35973 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nodemailer -- nodemailer	The package nodemailer before 6.6.1 are vulnerable to HTTP Header Injection if unsanitized user input that may contain newlines and carriage returns is passed into an address object.	2021-06-29	not yet calculated	CVE-2021-23400 MISC MISC MISC MISC
ntop -- ndpi	ntop nDPI 3.4 has a stack-based buffer overflow in processClientServerHello.	2021-07-01	not yet calculated	CVE-2021-36082 MISC MISC MISC
nvidia -- mb2	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow could cause memory corruption, which might lead to denial of service or code execution.	2021-06-30	not yet calculated	CVE-2021-34384 CONFIRM
nvidia -- mb2	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might lead to denial of service or escalation of privileges.	2021-06-30	not yet calculated	CVE-2021-34383 CONFIRM
nvidia -- mb2	Bootloader contains a vulnerability in NVIDIA MB2 where potential heap overflow might cause corruption of the heap metadata, which might lead to arbitrary code execution, denial of service, and information disclosure during secure boot.	2021-06-30	not yet calculated	CVE-2021-34380 CONFIRM
nvidia -- trusty	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 11 is missing. Improper restriction of operations within the bounds of a memory buffer might lead to information disclosure, denial of service, or escalation of privileges.	2021-06-30	not yet calculated	CVE-2021-34378 CONFIRM
nvidia -- trusty	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 9 is missing. Improper restriction of operations within the bounds of a memory buffer might lead to escalation of privileges, information disclosure, and denial of service.	2021-06-30	not yet calculated	CVE-2021-34377 CONFIRM
nvidia -- trusty	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 5 is missing. Improper restriction of operations within the bounds of a memory buffer might lead to denial of service, escalation of privileges, and information disclosure.	2021-06-30	not yet calculated	CVE-2021-34376 CONFIRM
nvidia -- trusty	Trusty contains a vulnerability in all trusted applications (TAs) where the stack cookie was not randomized, which might result in stack-based buffer overflow, leading to denial of service, escalation of privileges, and information disclosure.	2021-06-30	not yet calculated	CVE-2021-34375 CONFIRM
nvidia -- trusty	Trusty contains a vulnerability in command handlers where the length of input buffers is not verified. This vulnerability can cause memory corruption, which may lead to information disclosure, escalation of privileges, and denial of service.	2021-06-30	not yet calculated	CVE-2021-34374 CONFIRM
nvidia -- trusty	Trusty trusted Linux kernel (TLK) contains a vulnerability in the NVIDIA TLK kernel where a lack of heap hardening could cause heap overflows, which might lead to information disclosure and denial of service.	2021-06-30	not yet calculated	CVE-2021-34373 CONFIRM
nvidia -- trusty	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the calculation of a length could lead to a heap overflow.	2021-06-30	not yet calculated	CVE-2021-34385 CONFIRM
nvidia -- trusty	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 10 is missing. The length of an I/O buffer parameter is not checked, which might lead to memory corruption.	2021-06-30	not yet calculated	CVE-2021-34379 CONFIRM
nvidia -- trusty	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel function where a lack of checks allows the exploitation of an integer overflow on the size parameter of the tz_map_shared_mem function, which might lead to denial of service, information disclosure, or data tampering.	2021-06-30	not yet calculated	CVE-2021-34381 CONFIRM
nvidia -- trusty	Trusty TLK contains a vulnerability in the NVIDIA TLK kernelâ€™s tz_map_shared_mem function where an integer overflow on the size parameter causes the request buffer and the logging buffer to overflow, allowing writes to arbitrary addresses within the kernel.	2021-06-30	not yet calculated	CVE-2021-34382 CONFIRM
openthread -- wpantund	OpenThread wpantund through 2021-07-02 has a stack-based Buffer Overflow because of an inconsistency in the integer data type for metric_len.	2021-07-02	not yet calculated	CVE-2021-33889 MISC MISC CONFIRM
openvpn -- openvpn	OpenVPN before version 2.5.3 on Windows allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (openvpn.exe).	2021-07-02	not yet calculated	CVE-2021-3606 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openvpn -- openvpn_connect	OpenVPN Connect 3.2.0 through 3.3.0 allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (OpenVPNConnect.exe).	2021-07-02	not yet calculated	CVE-2021-3613 MISC
phpfusion -- phpfusion	A stored cross site scripting (XSS) vulnerability in /administration/settings_registration.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Registration" field.	2021-07-02	not yet calculated	CVE-2020-23184 MISC
phpfusion -- phpfusion	A stored cross site scripting (XSS) vulnerability in administration/settings_main.php of PHP-Fusion 9.03.50 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Site footer" field.	2021-07-02	not yet calculated	CVE-2020-23179 MISC
phpfusion -- phpfusion	An issue exists in PHP-Fusion 9.03.50 where session cookies are not deleted once a user logs out, allowing for an attacker to perform a session replay attack and impersonate the victim user.	2021-07-02	not yet calculated	CVE-2020-23178 MISC
phpfusion -- phpfusion	The component /php-fusion/infusions/shoutbox_panel/shoutbox_archive.php in PHP-Fusion 9.03.60 allows attackers to redirect victim users to malicious websites via a crafted payload entered into the Shoutbox message panel.	2021-07-02	not yet calculated	CVE-2020-23182 MISC
phpfusion -- phpfusion	A reflected cross site scripting (XSS) vulnerability in /administration/theme.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Manage Theme" field.	2021-07-02	not yet calculated	CVE-2020-23181 MISC
phpfusion -- phpfusion	A stored cross site scripting (XSS) vulnerability in /administration/setting_security.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-07-02	not yet calculated	CVE-2020-23185 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Configure categories" field under the "Categorise Lists" module.	2021-07-01	not yet calculated	CVE-2020-23214 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "List Description" field under the "Edit A List" module.	2021-07-01	not yet calculated	CVE-2020-23209 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in the "Import emails" module in phplist 3.5.4 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-07-02	not yet calculated	CVE-2020-23190 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Edit Values" field under the "Configure Attributes" module.	2021-07-01	not yet calculated	CVE-2020-23207 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add a list" field under the "Import Emails" module.	2021-07-01	not yet calculated	CVE-2020-23217 MISC MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the "Campaign" field under the "Send a campaign" module.	2021-07-02	not yet calculated	CVE-2020-36398 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the "rule1" parameter under the "Bounce Rules" module.	2021-07-02	not yet calculated	CVE-2020-36399 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Send test" field under the "Start or continue campaign" module.	2021-07-01	not yet calculated	CVE-2020-23208 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload in the "admin" parameter under the "Manage administrators" module.	2021-07-02	not yet calculated	CVE-2020-23192 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in the "Import Subscribers" feature in phplist 3.5.4 and below allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-07-02	not yet calculated	CVE-2020-23194 MISC
plizer -- scrutinizer	Plixer Scrutinizer 19.0.2 is affected by: SQL Injection. The impact is: obtain sensitive information (remote).	2021-06-30	not yet calculated	CVE-2021-28993 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
powermux -- powermux	PowerMux is a drop-in replacement for Go's http.ServeMux. In PowerMux versions prior to 1.1.1, attackers may be able to craft phishing links and other open redirects by exploiting the trailing slash redirection feature. This may lead to users being redirected to untrusted sites after following an attacker crafted link. The issue is resolved in v1.1.1. There are no existing workarounds.	2021-06-29	not yet calculated	CVE-2021-32721 CONFIRM
project_acrn -- acrn-hypervisor	ACRN before 2.5 has a devicemodel/hw/pci/xhci.c NULL Pointer Dereference for a trb pointer.	2021-07-02	not yet calculated	CVE-2021-36146 MISC
project_acrn -- acrn-hypervisor	ACRN before 2.5 has a hw/pci/virtio/virtio.c vq_endchains NULL Pointer Dereference.	2021-07-02	not yet calculated	CVE-2021-36143 MISC
project_acrn -- acrn-hypervisor	An issue was discovered in ACRN before 2.5. It allows a devicemodel/hw/pci/virtio/virtio_net.c virtio_net_ping_rxq NULL pointer dereference for vq->used.	2021-07-02	not yet calculated	CVE-2021-36147 MISC
project_acrn -- acrn-hypervisor	An issue was discovered in ACRN before 2.5. dmar_free_irte in hypervisor/arch/x86/vtd.c allows an irte_alloc_bitmap buffer overflow.	2021-07-02	not yet calculated	CVE-2021-36148 MISC
project_acrn -- acrn-hypervisor	The Device Model in ACRN through 2.5 has a devicemodel/core/mem.c use-after-free for a freed rb_entry.	2021-07-02	not yet calculated	CVE-2021-36145 MISC
project_acrn -- acrn-hypervisor	The polling timer handler in ACRN before 2.5 has a use-after-free for a freed virtio device, related to devicemodel/hw/pci/virtio/*.c.	2021-07-02	not yet calculated	CVE-2021-36144 MISC
qnap - qts_and_quts_hero	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217.	2021-07-01	not yet calculated	CVE-2021-28804 CONFIRM
qnap -- nas_devices	A stored XSS vulnerability has been reported to affect QNAP NAS running QuLog Center. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QuLog Center versions prior to 1.2.0.	2021-07-01	not yet calculated	CVE-2020-36196 CONFIRM
qnap -- nas_devices	An XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.2.1566 Build 20210202. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 build 20210414. This issue does not affect: QNAP Systems Inc. QTS 4.5.3.	2021-07-01	not yet calculated	CVE-2020-36194 CONFIRM
qnap -- q'center	This issue affects: QNAP Systems Inc. Q'center versions prior to 1.11.1004.	2021-07-01	not yet calculated	CVE-2021-28803 CONFIRM
qnap -- qts_and_quts_hero	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217.	2021-07-01	not yet calculated	CVE-2021-28802 CONFIRM
rarlab -- unrar	UnRAR 5.6.1.7 through 5.7.4 and 6.0.3 has an out-of-bounds write during a memcpy in QuickOpen::ReadRaw when called from QuickOpen::ReadNext.	2021-07-01	not yet calculated	CVE-2018-25018 MISC MISC MISC
rarlab -- unrar	UnRAR 5.6.1.2 and 5.6.1.3 has a heap-based buffer overflow in Unpack::CopyString (called from Unpack::Unpack5 and CmdExtract::ExtractCurrentFile).	2021-07-01	not yet calculated	CVE-2017-20006 MISC MISC MISC
ratpack -- ratpack	Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the client side session module uses the application startup time as the signing key by default. This means that if an attacker can determine this time, and if encryption is not also used (which is recommended, but is not on by default), the session data could be tampered with by someone with the ability to write cookies. The default configuration is unsuitable for production use as an application restart renders all sessions invalid and is not multi-host compatible, but its use is not actively prevented. As of Ratpack 1.9.0, the default value is a securely randomly generated value, generated at application startup time. As a workaround, supply an alternative signing key, as per the documentation's recommendation.	2021-06-29	not yet calculated	CVE-2021-29480 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ratpack -- ratpack	Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, a user supplied `X-Forwarded-Host` header can be used to perform cache poisoning of a cache fronting a Ratpack server if the cache key does not include the `X-Forwarded-Host` header as a cache key. Users are only vulnerable if they do not configure a custom `PublicAddress` instance. For versions prior to 1.9.0, by default, Ratpack utilizes an inferring version of `PublicAddress` which is vulnerable. This can be used to perform redirect cache poisoning where an attacker can force a cached redirect to redirect to their site instead of the intended redirect location. The vulnerability was patched in Ratpack 1.9.0. As a workaround, ensure that `ServerConfigBuilder::publicAddress` correctly configures the server in production.	2021-06-29	not yet calculated	CVE-2021-29479 MISC CONFIRM
ratpack -- ratpack	Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the default configuration of client side sessions results in unencrypted, but signed, data being set as cookie values. This means that if something sensitive goes into the session, it could be read by something with access to the cookies. For this to be a vulnerability, some kind of sensitive data would need to be stored in the session and the session cookie would have to leak. For example, the cookies are not configured with httpOnly and an adjacent XSS vulnerability within the site allowed capture of the cookies. As of version 1.9.0, a securely randomly generated signing key is used. As a workaround, one may supply an encryption key, as per the documentation recommendation.	2021-06-29	not yet calculated	CVE-2021-29481 MISC CONFIRM
ratpack -- ratpack	Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, a malicious attacker can achieve Remote Code Execution (RCE) via a maliciously crafted Java deserialization gadget chain leveraged against the Ratpack session store. If one's application does not use Ratpack's session mechanism, it is not vulnerable. Ratpack 1.9.0 introduces a strict allow-list mechanism that mitigates this vulnerability when used. Two possible workarounds exist. The simplest mitigation for users of earlier versions is to reduce the likelihood of attackers being able to write to the session data store. Alternatively or additionally, the allow-list mechanism could be manually back ported by providing an alternative implementation of `SessionSerializer` that uses an allow-list.	2021-06-29	not yet calculated	CVE-2021-29485 MISC CONFIRM
rawspeed -- rawspeed	RawSpeed (aka librawspeed) 3.1 has a heap-based buffer overflow in TableLookUp::setTable.	2021-07-01	not yet calculated	CVE-2018-25017 MISC MISC MISC
record-like-deep-assign -- record-like-deep-assign	All versions of package record-like-deep-assign are vulnerable to Prototype Pollution via the main functionality.	2021-07-02	not yet calculated	CVE-2021-23402 CONFIRM CONFIRM
samtools -- htslib	HTSlib 1.10 through 1.10.2 allows out-of-bounds write access in vcf_parse_format (called from vcf_parse and vcf_read).	2021-07-01	not yet calculated	CVE-2020-36403 MISC MISC MISC
selinux_project -- selinux	The CIL compiler in SELinux 3.2 has a use-after-free in cil_reset_classpermission (called from cil_reset_classperms_set and cil_reset_classperms_list).	2021-07-01	not yet calculated	CVE-2021-36086 MISC MISC MISC
selinux_project -- selinux	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __verify_map_perm_classperms and hashtab_map).	2021-07-01	not yet calculated	CVE-2021-36085 MISC MISC MISC
selinux_project -- selinux	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __cil_verify_classpermission and __cil_pre_verify_helper).	2021-07-01	not yet calculated	CVE-2021-36084 MISC MISC MISC
selinux_project -- selinux	The CIL compiler in SELinux 3.2 has a heap-based buffer over-read in ebitmap_match_any (called indirectly from cil_check_neverallow). NOTE: bad0a746e9f4cf260dedba5828d9645d50176aac is cited in the OSV "fixed" field but does not have a code change.	2021-07-01	not yet calculated	CVE-2021-36087 MISC MISC MISC
seromq -- libzmq	ZeroMQ libzmq 4.3.3 has a heap-based buffer overflow in zmq::tcp_read, a different vulnerability than CVE-2021-20235.	2021-07-01	not yet calculated	CVE-2020-36400 MISC MISC MISC
sita -- azurcms	A SQL injection vulnerability in azurWebEngine in Sita AzurCMS through 1.2.3.12 allows an authenticated attacker to execute arbitrary SQL commands via the id parameter to mesdocs.ajax.php in azurWebEngine/eShop. By default, the query is executed as DBA.	2021-07-02	not yet calculated	CVE-2021-27950 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sloan -- smartfaucets	There exists an unauthenticated BLE Interface in Sloan SmartFaucets including Optima EAF, Optima ETF/EBF, BASYS EFX, and Flushometers including SOLIS. The vulnerability allows for unauthenticated kinetic effects and information disclosure on the faucets. It is possible to use the Bluetooth Low Energy (BLE) connectivity to read and write to many BLE characteristics on the device. Some of these control the flow of water, the sensitivity of the sensors, and information about maintenance.	2021-06-30	not yet calculated	CVE-2021-20107 MISC
sourcecodester -- phone_shop_sales_managements_system	Sourcecodester Phone Shop Sales Managements System 1.0 is vulnerable to Insecure Direct Object Reference (IDOR). Any attacker will be able to see the invoices of different users by changing the id parameter.	2021-07-01	not yet calculated	CVE-2021-35337 MISC
stellar -- js-stellar-sdk	js-stellar-sdk is a Javascript library for communicating with a Stellar Horizon server. The `Utils.readChallengeTx` function used in SEP-10 Stellar Web Authentication states in its function documentation that it reads and validates the challenge transaction including verifying that the `serverAccountID` has signed the transaction. In js-stellar-sdk before version 8.2.3, the function does not verify that the server has signed the transaction. Applications that also used `Utils.verifyChallengeTxThreshold` or `Utils.verifyChallengeTxSigners` to verify the signatures including the server signature on the challenge transaction are unaffected as those functions verify the server signed the transaction. Applications calling `Utils.readChallengeTx` should update to version 8.2.3, the first version with a patch for this vulnerability, to ensure that the challenge transaction is completely valid and signed by the server creating the challenge transaction.	2021-07-02	not yet calculated	CVE-2021-32738 CONFIRM MISC
stormshield -- stormshield	An issue was discovered in Stormshield SNS through 4.2.1. A brute-force attack can occur.	2021-07-01	not yet calculated	CVE-2021-28127 MISC MISC
sulu -- sulu	Sulu is an open-source PHP content management system based on the Symfony framework. In versions of Sulu prior to 1.6.41, it is possible for a logged in admin user to add a script injection (cross-site-scripting) in the collection title. The problem is patched in version 1.6.41. As a workaround, one may manually patch the affected JavaScript files in lieu of updating.	2021-07-02	not yet calculated	CVE-2021-32737 CONFIRM MISC
suse -- linux_enterprise_server	A UNIX Symbolic Link (Symlink) Following vulnerability in arpwatch of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Factory, Leap 15.2 allows local attackers with control of the runtime user to run arpwatch as to escalate to root upon the next restart of arpwatch. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS arpwatch versions prior to 2.1a15. SUSE Manager Server 4.0 arpwatch versions prior to 2.1a15. SUSE OpenStack Cloud Crowbar 9 arpwatch versions prior to 2.1a15. openSUSE Factory arpwatch version 2.1a15-169.5 and prior versions. openSUSE Leap 15.2 arpwatch version 2.1a15-lp152.5.5 and prior versions.	2021-06-30	not yet calculated	CVE-2021-25321 CONFIRM
suse -- linux_enterprise_server	A Use of Password Hash Instead of Password for Authentication vulnerability in cryptctl of SUSE Linux Enterprise Server for SAP 12-SP5, SUSE Manager Server 4.0 allows attackers with access to the hashed password to use it without having to crack it. This issue affects: SUSE Linux Enterprise Server for SAP 12-SP5 cryptctl versions prior to 2.4. SUSE Manager Server 4.0 cryptctl versions prior to 2.4.	2021-06-30	not yet calculated	CVE-2019-18906 CONFIRM
symantec -- advanced_secure_gateway	The Symantec Advanced Secure Gateway (ASG) and ProxySG web management consoles are susceptible to an authentication bypass vulnerability. An unauthenticated attacker can execute arbitrary CLI commands, view/modify the appliance configuration and policy, and shutdown/restart the appliance.	2021-06-30	not yet calculated	CVE-2021-30648 MISC
synacor -- zimbra_collaboration_suite	An issue was discovered in ProxyServlet.java in the /proxy servlet in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.x before 9.0.0 Patch 16. The value of the X-Host header overwrites the value of the Host header in proxied requests. The value of X-Host header is not checked against the whitelist of hosts Zimbra is allowed to proxy to (the zimbraProxyAllowedDomains setting).	2021-07-02	not yet calculated	CVE-2021-35209 MISC MISC MISC MISC
synacor -- zimbra_collaboration_suite	An issue was discovered in ZmMailMsgView.js in the Calendar Invite component in Zimbra Collaboration Suite 8.8.x before 8.8.15 Patch 23. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.	2021-07-02	not yet calculated	CVE-2021-35208 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synacor -- zimbra_collaboration_suite	An issue was discovered in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.0 before 9.0.0 Patch 16. An XSS vulnerability exists in the login component of Zimbra Web Client, in which an attacker can execute arbitrary JavaScript by adding executable JavaScript to the loginErrorCode parameter of the login url.	2021-07-02	not yet calculated	CVE-2021-35207 MISC MISC MISC MISC
synacor -- zimbra_collaboration_suite	An open redirect vulnerability exists in the /preauth Servlet in Zimbra Collaboration Suite through 9.0. To exploit the vulnerability, an attacker would need to have obtained a valid zimbra auth token or a valid preauth token. Once the token is obtained, an attacker could redirect a user to any URL via isredirect=1&redirectURL= in conjunction with the token data (e.g., a valid authtoken= value).	2021-07-02	not yet calculated	CVE-2021-34807 MISC MISC MISC MISC
teachers_record_management_system -- teachers_record_managemet_system	Multiple SQL Injection vulnerabilities in Teachers Record Management System 1.0 allow remote authenticated users to execute arbitrary SQL commands via the 'editid' GET parameter in edit-subjects-detail.php, edit-teacher-detail.php, or the 'searchdata' POST parameter in search.php.	2021-07-01	not yet calculated	CVE-2021-28423 MISC MISC MISC MISC
teachers_record_management_system -- teachers_record_managemet_system	A stored cross-site scripting (XSS) vulnerability in Teachers Record Management System 1.0 allows remote authenticated users to inject arbitrary web script or HTML via the 'email' POST parameter in adminprofile.php.	2021-07-01	not yet calculated	CVE-2021-28424 MISC MISC MISC MISC
tensorflow -- tensorflow	** DISPUTED ** TensorFlow through 2.5.0 allows attackers to overwrite arbitrary files via a crafted archive when tf.keras.utils.get_file is used with extract=True. NOTE: the vendor's position is that tf.keras.utils.get_file is not intended for untrusted archives.	2021-06-30	not yet calculated	CVE-2021-35958 MISC MISC MISC MISC MISC
tesseract_ocr -- tesseract	Tesseract OCR 5.0.0-alpha-20201231 has a one_ell_conflict use-after-free during a strpbrk call.	2021-07-01	not yet calculated	CVE-2021-36081 MISC MISC MISC
think-js -- think-helper	think-helper defines a set of helper functions for ThinkJS. In versions of think-helper prior to 1.1.3, the software receives input from an upstream component that specifies attributes that are to be initialized or updated in an object, but it does not properly control modifications of attributes of the object prototype. The vulnerability is patched in version 1.1.3.	2021-06-30	not yet calculated	CVE-2021-32736 CONFIRM
tibco -- multiple products	The Windows Installation component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Statistics Services, TIBCO Spotfire Statistics Services, and TIBCO Spotfire Statistics Services contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition: versions 1.2.4 and below, TIBCO Enterprise Runtime for R - Server Edition: versions 1.3.0 and 1.3.1, TIBCO Enterprise Runtime for R - Server Edition: versions 1.4.0, 1.5.0, and 1.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.3.0 and below, TIBCO Spotfire Server: versions 10.3.12 and below, TIBCO Spotfire Server: versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, 10.10.1, 10.10.2, 10.10.3, and 10.10.4, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, and 11.3.0, TIBCO Spotfire Statistics Services: versions 10.3.0 and below, TIBCO Spotfire Statistics Services: versions 10.10.0, 10.10.1, and 10.10.2, and TIBCO Spotfire Statistics Services: versions 11.1.0, 11.2.0, and 11.3.0.	2021-06-29	not yet calculated	CVE-2021-23275 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tibco -- multiple products	The TIBCO Spotfire Server and TIBCO Enterprise Runtime for R components of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Statistics Services, TIBCO Spotfire Statistics Services, and TIBCO Spotfire Statistics Services contain a vulnerability that theoretically allows a low privileged attacker with local access on the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from the affected component searching for run-time artifacts outside of the installation hierarchy. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition: versions 1.2.4 and below, TIBCO Enterprise Runtime for R - Server Edition: versions 1.3.0 and 1.3.1, TIBCO Enterprise Runtime for R - Server Edition: versions 1.4.0, 1.5.0, and 1.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.3.0 and below, TIBCO Spotfire Server: versions 10.3.12 and below, TIBCO Spotfire Server: versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, 10.10.1, 10.10.2, 10.10.3, and 10.10.4, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, and 11.3.0, TIBCO Spotfire Statistics Services: versions 10.3.0 and below, TIBCO Spotfire Statistics Services: versions 10.10.0, 10.10.1, and 10.10.2, and TIBCO Spotfire Statistics Services: versions 11.1.0, 11.2.0, and 11.3.0.	2021-06-29	not yet calculated	CVE-2021-28830 CONFIRM CONFIRM
tieline -- ip_audio_gateway	Tieline IP Audio Gateway 2.6.4.8 and below is affected by Incorrect Access Control. A vulnerability in the Tieline Web Administrative Interface could allow an unauthenticated user to access a sensitive part of the system with a high privileged account.	2021-07-01	not yet calculated	CVE-2021-35336 MISC
torproject -- tor	An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-006. The v3 onion service descriptor parsing allows out-of-bounds memory access, and a client crash, via a crafted onion service descriptor	2021-06-29	not yet calculated	CVE-2021-34550 MISC CONFIRM
torproject -- tor	An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-005. Hashing is mishandled for certain retrieval of circuit data. Consequently. an attacker can trigger the use of an attacker-chosen circuit ID to cause algorithm inefficiency.	2021-06-29	not yet calculated	CVE-2021-34549 MISC CONFIRM
torproject -- tor	An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-003. An attacker can forge RELAY_END or RELAY_RESOLVED to bypass the intended access control for ending a stream.	2021-06-29	not yet calculated	CVE-2021-34548 MISC CONFIRM
ts-nodash -- ts-nodash	All versions of package ts-nodash are vulnerable to Prototype Pollution via the Merge() function due to lack of validation input.	2021-07-02	not yet calculated	CVE-2021-23403 MISC MISC
unetworking -- uwebsockets	uWebSockets 18.11.0 and 18.12.0 has a stack-based buffer overflow in uWS::TopicTree::trimTree (called from uWS::TopicTree::unsubscribeAll).	2021-07-01	not yet calculated	CVE-2020-36406 MISC MISC MISC
veeam -- veeam	Veeam Backup and Replication 10 before 10.0.1.4854 P20210609 and 11 before 11.0.0.837 P20210507 mishandles deserialization during Microsoft .NET remoting.	2021-06-30	not yet calculated	CVE-2021-35971 MISC MISC
western_digital -- multiple_products	Western Digital WD My Book Live (2.x and later) and WD My Book Live Duo (all versions) have an administrator API that can perform a system factory restore without authentication, as exploited in the wild in June 2021, a different vulnerability than CVE-2018-18472.	2021-06-29	not yet calculated	CVE-2021-35941 MISC MISC
xen -- xen	Guest triggered use-after-free in Linux xen-netback A malicious or buggy network PV frontend can force Linux netback to disable the interface and terminate the receive kernel thread associated with queue 0 in response to the frontend sending a malformed packet. Such kernel thread termination will lead to a use-after-free in Linux netback when the backend is destroyed, as the kernel thread associated with queue 0 will have already exited and thus the call to kthread_stop will be performed against a stale pointer.	2021-06-29	not yet calculated	CVE-2021-28691 MISC
xen -- xen	x86: TSX Async Abort protections not restored after S3 This issue relates to the TSX Async Abort speculative security vulnerability. Please see https://xenbits.xen.org/xsa/advisory-305.html for details. Mitigating TAA by disabling TSX (the default and preferred option) requires selecting a non-default setting in MSR_TSX_CTRL. This setting isn't restored after S3 suspend.	2021-06-29	not yet calculated	CVE-2021-28690 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xen -- xen	xen/arm: Boot modules are not scrubbed The bootloader will load boot modules (e.g. kernel, initramfs...) in a temporary area before they are copied by Xen to each domain memory. To ensure sensitive data is not leaked from the modules, Xen must "scrub" them before handing the page over to the allocator. Unfortunately, it was discovered that modules will not be scrubbed on Arm.	2021-06-30	not yet calculated	CVE-2021-28693 MISC
xen -- xen	inappropriate x86 IOMMU timeout detection / handling IOMMUs process commands issued to them in parallel with the operation of the CPU(s) issuing such commands. In the current implementation in Xen, asynchronous notification of the completion of such commands is not used. Instead, the issuing CPU spin-waits for the completion of the most recently issued command(s). Some of these waiting loops try to apply a timeout to fail overly-slow commands. The course of action upon a perceived timeout actually being detected is inappropriate: - on Intel hardware guests which did not originally cause the timeout may be marked as crashed, - on AMD hardware higher layer callers would not be notified of the issue, making them continue as if the IOMMU operation succeeded.	2021-06-30	not yet calculated	CVE-2021-28692 MISC
xml2dict -- xml2dict	XXE vulnerability in 'XML2Dict' version 0.2.2 allows an attacker to cause a denial of service.	2021-06-30	not yet calculated	CVE-2021-25951 MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A cross-site request forgery vulnerability exists in versions prior to 12.10.5, and in versions 13.0 through 13.1. It's possible for forge an URL that, when accessed by an admin, will reset the password of any user in XWiki. The problem has been patched in XWiki 12.10.5 and 13.2RC1. As a workaround, it is possible to apply the patch manually by modifying the `register_macros.vm` template.	2021-07-01	not yet calculated	CVE-2021-32730 CONFIRM MISC MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Between (and including) versions 13.1RC1 and 13.1, the reset password form reveals the email address of users just by giving their username. The problem has been patched on XWiki 13.2RC1. As a workaround, it is possible to manually modify the `resetpasswordinline.vm` to perform the changes made to mitigate the vulnerability.	2021-07-01	not yet calculated	CVE-2021-32731 MISC CONFIRM MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A vulnerability exists in versions prior to 12.6.88, 12.10.4, and 13.0. The script service method used to reset the authentication failures record can be executed by any user with Script rights and does not require Programming rights. An attacher with script rights who is able to reset the authentication failure record might perform a brute force attack, since they would be able to virtually deactivate the mechanism introduced to mitigate those attacks. The problem has been patched in version 12.6.8, 12.10.4 and 13.0. There are no workarounds aside from upgrading.	2021-07-01	not yet calculated	CVE-2021-32729 CONFIRM MISC
zoho -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus before 6104, in rare situations, allows attackers to obtain sensitive information about the password-sync database application.	2021-07-02	not yet calculated	CVE-2021-31874 MISC
zoho -- manageengine_applications_manager	Zoho ManageEngine Applications Manager before 15130 is vulnerable to Stored XSS while importing malicious user details (e.g., a crafted user name) from AD.	2021-07-01	not yet calculated	CVE-2021-31813 MISC
zyxel -- firmware	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device.	2021-07-02	not yet calculated	CVE-2021-35029 MISC

Back to top